UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,380	10/31/2003	Stephen M. Trimberger	X-1435 US	1825

24309 7590 07/09/2009

XILINX, INC
ATTN: LEGAL DEPARTMENT
2100 LOGIC DR
SAN JOSE, CA 95124

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
07/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/714,380	TRIMBERGER, STEPHEN M.	
	Examiner	Art Unit	
	RANDAL D. MORAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-16,18-20 and 22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-16,18-20 and 22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-3, 5-16, 19, 20 and 22 are pending.

This Office Action in response to amendment filed 4/15/2009.

Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. **Claims 1-3, 5-16, 18-20 and 22** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Pang et al. (US 6,981,153)**, hereafter "Pang" in view of **Lesea et al. (US 6,496,971),** hereafter "Lesea" in view of **Weinlander (US 5,991,858)**, hereafter "Weinlander".

Considering **Claim 1,** Burnham discloses a system of securely using decryption keys during Programmable Logic Device (PLD) configuration (column 2- lines 35-45), comprises:

a key storage register coupled to the microcontroller for storing key data (Fig. 10A, column 15, lines 14-23, Lesea- column 4- lines 17-24); a decryptor coupled to the key storage register (Fig. 3- item 24), wherein only the decryptor can read from the key storage register (column 13- lines 37-56, column 16- lines 27-33, Fig. 8, Fig. 9); and a configuration data register in the PLD (Fig. 3, column 11- lines 44-56), wherein the configuration data register cannot be read by the microcontroller after the decryptor is used (column 14- lines 18-38), and disallows the microcontroller access to the key storage register by blocking the signal path coupling the microcontroller and the key storage register (column 14- lines 18-38).

Pang does not explicitly disclose a microcontroller within the PLD for receiving an encrypted bitstream.

Lesea discloses a microcontroller within the PLD for receiving an encrypted bitstream (column 4- lines 12-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Pang by a microcontroller within the PLD for receiving an encrypted bitstream as taught by Lesea in order to support multiple configuration modes (Lesea- column 2- lines 57-58).

The combination does not explicitly disclose the decryptor is a software decryptor stored in a memory and executed by the microcontroller, wherein the system further comprises hardware that selectively enables access to the key storage register by allowing the microcontroller access when a program counter of the microcontroller specifies an address within an address range corresponding to the software decryptor within the memory.

Weinlander discloses the decryptor is a software decryptor stored in a memory and executed by the microcontroller, wherein the system further comprises hardware that selectively

enables access to the key storage register by allowing the microcontroller access when a program counter of the microcontroller specifies an address within an address range corresponding to the software decryptor within the memory (column 6- lines 5-12).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination by hardware that selectively enables access to the key storage register by allowing the microcontroller access when a program counter of the microcontroller specifies an address within an address range corresponding to the software decryptor within the memory in order to provide further safegaurds in data protection (Weinlander- column 4- lines 20-31).

Considering **Claim 2,** the combination discloses the microcontroller stores key data in the key storage register, but the microcontroller cannot read from the key storage register (Pang- column 15- lines 39-40 and 58-66, column 16- lines 27-33).

Considering **Claim 3,** the combination discloses the decryptor is a hardware decryptor embedded in an integrated circuit along with the PLD (Pang- column 13- lines 37-56, Fig. 3- item 24).

Considering **Claims 5, 10,** the combination discloses the memory is a ROM having a decryption engine (Lesea- column 3- lines 7-12, column 4– lines 17-25).

Considering **Claim 6,** the combination discloses the microcontroller further receives a configuration boot program comprising the decryptor in programmatic form along with the encrypted bitstream comprising encrypted configuration data to be loaded into the configuration data register (Lesea- column 8- lines 33-55, Pang- column 1- lines 31-38 and 52-58).

Considering **Claim 7,** the combination discloses the microcontroller, the key register, the decryptor, and the configuration data register are all within the PLD (Pang- Fig. 3).

Considering **Claim 8,** the combination discloses the microcontroller is an emulated microcontroller in the PLD (Pang- column 5- lines 47-64).

Considering **Claim 9,** the combination discloses a system of securely using decryption keys during configuration of an integrated circuit having programmable logic (Pamg- abstract, column 2- lines 35-45), comprising: a microcontroller within the integrated circuit for receiving an encrypted bitstream (Lesea- column 4- lines 15-25, Pang- column 5- lines 47-64); a key storage register coupled to the microcontroller for storing key data (Pang- Fig. 10A, column 15, lines 14-23); a decryption program stored in a memory that uses a predetermined memory address to enable access to the key storage register (Pang- column 12- lines 36-47); and a configuration data register in the integrated circuit (Pang- Fig. 3, column 11- lines 44-56), wherein the configuration data register cannot be read by the microcontroller after the decryption program is used (Pang- column 11- lines 44-56, column 14- lines 18-38); wherein access to the key storage register by the microcontroller is allowed only when a program counter of the microcontroller specifies an address within an address range corresponding to the decryption program in the memory (Weinlander- column 6- lines 5-12) wherein access to the key storage register by the microcontroller is disallowed when the program counter of the microcontroller specifies an address outside of an address range corresponding to the decryption program in the memory (Weinlander- column 6- lines 5-12) by blocking the signal path coupling the microcontroller and the key storage register (Pang -column 14- lines 18-38).

Considering **Claim 11,** the combination discloses the microcontroller further receives a configuration boot program along with the encrypted bitstream (Lesea- column 8- lines 32-55).

Considering **Claim 12,** the combination discloses a method of securely using decryption keys during field programmable gate array configuration (Pang- abstract- column 2- lines 35-45), comprising the steps of: receiving an encrypted bitstream at a microcontroller within the field programmable gate array (Lesea- column 4- lines 15-25, Pang- column 5- lines 47-64); loading a decryptor with data from a key register (Pang- column 13- lines 37-55); loading the decryptor with data from the microcontroller (Pang- column 13- lines 37-56); and loading a configuration data register with a decrypted bitstream from the decryptor (Pang- column 14- lines 18-38), wherein the configuration data register cannot be read by the microcontroller after the decryptor is used (Pang- column 14- lines 18-38) selectively enables access to the key storage register by allowing the microcontroller access when a program counter of the microcontroller specifies an address within an address range corresponding to the software decryptor within the memory (Weinlander- column 6- lines 5-12) disabling access to the key register by blocking the signal path coupling the microcontroller and the key register (Pang- column 14- lines 18-38) when the program counter of the microcontroller specifies an address outside of the address range of the decryptor (Weinlander- column 6- lines 5-12).

Considering **Claim 13,** the combination discloses the step of loading the key register with key data from the microcontroller (Pang- column 15- lines 39-40 and 58-66).

Considering **Claim 14,** the combination discloses the configuration data register cannot be read by the microcontroller while the decryptor is used (Pang- column 14- lines 18-33).

Considering **Claim 15,** the combination discloses the microcontroller cannot read from the key register (Pang- column 15- lines 39-40 and 58-66, column 16- lines 27-33).

Considering **Claim 16,** the combination discloses only the decryptor can read from the key storage register (Pang- column 13- lines 37-55, column 15- lines 59-66, column 16- lines 27-33).

Considering **Claim 18,** the combination discloses a system of securely using decryption keys during programmable logic device configuration (Pang- abstract, column 2- lines 35-45), comprises: a memory-mapped key register coupled to a microcontroller data bus (Pang- column 15- lines 14-23); a decryptor engine stored in non-volatile memory and coupled to the microcontroller data bus (Pang- column 13- lines 37-55); and logic circuitry limiting access to the key register from the microcontroller data bus using specified addresses of the non-volatile memory corresponding to the decryptor engine and a received program counter value of a microcontroller (Weinlander- column 6- lines 5-12). wherein the logic circuitry selectively blocks or unblocks a signal path coupling the microcontroller data bus and the key register (Pang- column 14- lines 18-38) according to the specified addresses of the non-volatile memory corresponding to the decryptor engine and the program counter value (Weinlander- column 6- lines 5-12).

Considering **Claim 19,** the combination does not explicitly disclose the logic circuitry uses specified addresses of the non-volatile memory by limiting access to minimum and

maximum ROM memory addresses using the microcontroller program counter (Weinlander- column 6- lines 5-12).

Consdering **Claim 20,** the combination discloses a computer-readable usable medium comprising instructions written thereon in the form of a bitstream that configures a programmable logic device (Pang- abstract, column 2- lines 35-45), the computer- readable usable medium comprising: a configuration boot program portion of the bitstream that runs a microcontroller on the programmable logic device (Lesea- column 8- lines 32-55); and an encrypted bitstream portion of the bitstream containing encrypted configuration data that when decrypted and loaded into a configuration data register on the programmable logic device configures the programmable logic device (Lesea- column 8- lines 33-55, Pang- column 2- lines 35-45), wherein the configuration boot program further comprises instructions for a decryptor (Pang- column 13- lines 37-56), wherein the configuration boot program stores the instructions for the decryptor Pang- column 2- lines 35-45), selectively enables access to the key storage register by allowing the microcontroller access when a program counter of the microcontroller specifies an address within an address range corresponding to the software decryptor within the memory (Weinlander- column 6- lines 5-12).

Considering **Claim 22,** the discloses the configuration boot program comprises instructions for a decompressor (Lesea- column 2- lines 12-25, column 8- lines 15-20).

Response to Arguments

Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e.,disallows the microcontroller access to the key storage register by blocking the signal path coupling the microcontroller and the key storage register) were not recited in the previously rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/R. D. M./
Examiner, Art Unit 2135
7/5/2009

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135